

1 **In the Claims**

2 No claims have been cancelled or added.

3 Claim 30 has been amended.

4 Claims 1-48 remain in the application and are listed as follows:

5

6 1. (Original) In a paging operating system having physical memory for
7 holding information and secondary storage comprising a page file for receiving
8 information that is paged out from the physical memory, a computer-implemented
9 method of protecting information comprising:

10 encrypting information using a key that is page-locked in the physical
11 memory; and

12 paging out, to the page file, the encrypted information.

13

14 2. (Original) The computer-implemented method of claim 1 further
15 comprising prior to said encrypting, creating the key and page locking the key in
16 the physical memory.

17

18 3. (Original) The computer-implemented method of claim 2, wherein
19 said creating the key comprises creating the key during system boot up.

20

21 4. (Original) The computer-implemented method of claim 2, wherein
22 said creating the key comprises generating a random key with a random key
23 generator.

1 5. (Original) The computer-implemented method of claim 4, wherein
2 said generating comprises using RSA RC4 as an encryption algorithm to generate
3 the key.

4
5 6. (Original) The computer-implemented method of claim 1, wherein
6 said encrypting comprises:

7 calling an operating system kernel;

8 the kernel using the page-locked key to encrypt the information.

9
10 7. (Original) The computer-implemented method of claim 6, wherein
11 said calling is performed by an application.

12
13 8. (Original) The computer-implemented method of claim 6, wherein
14 said calling is performed by an operating system memory manager.

15
16 9. (Original) One or more computer-readable media having computer-
17 readable instructions thereon which, when executed by a computer, perform the
18 computer-implemented method of claim 1.

19
20 10. (Original) An operating system programmed with instructions
21 which, when implemented by the operating system, implement the method of
22 claim 1.

23
24 11. (Original) In a paging operating system having main memory for
25 holding information and secondary storage comprising a page file for receiving

1 information that is paged out from the main memory, a computer-implemented
2 method of protecting information comprising:

3 page-locking a key in main memory;
4 restricting access to the page-locked key to only the operating system
5 kernel;
6 calling the operating system kernel to encrypt information;
7 accessing the page-locked key with the operating system kernel; and
8 using the operating system kernel to encrypt the information with the page-
9 locked key.

10
11 12. (Original) The computer-implemented method of claim 11, wherein
12 said calling is performed by an operating system memory manager.

13
14 13. (Original) The computer-implemented method of claim 11, wherein
15 said calling is performed by an application.

16
17 14. (Original) The computer-implemented method of claim 11 further
18 comprising prior to said calling:

19 designating at least one page in the main memory with a designation;
20 recognizing the designation and, responsive thereto, calling the operating
21 system kernel to encrypt the information.

22
23 15. (Original) The computer-implemented method of claim 14, wherein
24 said recognizing is performed by the memory manager.

1 16. (Original) The computer-implemented method of claim 11, wherein
2 said calling comprises specifying a memory location and a memory size associated
3 with the information to be encrypted.
4

5 17. (Original) One or more computer-readable media having computer-
6 readable instructions thereon which, when executed by a computer, perform the
7 computer-implemented method of claim 11.
8

9 18. (Original) An operating system programmed with instructions
10 which, when implemented by the operating system, implement the method of
11 claim 11.
12

13 19. (Original) In a paging operating system having main memory for
14 holding information and secondary storage comprising a page file for receiving
15 information that is paged out from the main memory, a computer-implemented
16 method of handling encrypted information comprising:

17 accessing encrypted information in the page file; and
18 decrypting the encrypted information with a key that is page-locked in the
19 main memory.
20

21 20. (Original) The computer-implemented method of claim 19 further
22 comprising placing the decrypted information in a page of main memory.
23

24 21. (Original) The computer-implemented method of claim 19 further
25 comprising placing the decrypted information in a page-locked page of main
memory.

1
2 22. (Original) The computer-implemented method of claim 19, wherein
3 the page-locked key is accessible only to the operating system kernel.
4

5 23. (Original) One or more computer-readable media having computer-
6 readable instructions thereon which, when executed by a computer, perform the
7 computer-implemented method of claim 19.
8

9 24. (Original) An operating system programmed with instructions
10 which, when implemented by the operating system, implement the method of
11 claim 19.
12

13 25. (Original) In a paging operating system having main memory for
14 holding information and secondary storage comprising a page file for receiving
15 information that is paged out from the main memory, a computer-implemented
16 method of protecting information comprising:

17 allocating a non-pageable page of main memory;

18 generating a random key; and

19 storing the random key in the non-pageable page of main memory, the
20 random key being configured for use by the operating system to encrypt
21 information that might be paged out to the page file.
22

23 26. (Original) The computer-implemented method of claim 25, wherein
24 said generating comprises using an RSA RC4 encryption algorithm.
25

1 27. (Original) The computer-implemented method of claim 25, wherein
2 said allocating takes place during system boot.

3
4 28. (Original) One or more computer-readable media having computer-
5 readable instructions thereon which, when executed by a computer, perform the
6 computer-implemented method of claim 25.

7
8 29. (Original) An operating system programmed with instructions
9 which, when implemented by the operating system, implement the method of
10 claim 25.

11
12 30. (Currently Amended) In an operating system having main memory
13 for holding information and secondary storage for receiving information that is
14 transferred out of main memory, a computer-implemented method of protecting
15 information comprising:

16 generating at least one non-pageable random key by using a random key
17 generation process;

18 encrypting at least one selected block of information in the main memory
19 with a software component that uses the at least one random key for encryption;

20 transferring the one encrypted block of information to the secondary
21 storage;

22 decrypting the one encrypted block of information with the software
23 component that uses the at least one random key for decryption; and

24 placing the decrypted block of information in the main memory.
25

1 31. (Original) The computer-implemented method of claim 30, wherein
2 said generating is performed during system boot up.

3
4 32. (Original) The computer-implemented method of claim 30 further
5 comprising restricting access to the at least one random key to only the software
6 component.

7
8 33. (Original) The computer-implemented method of claim 30, wherein
9 the software component comprises the operating system's kernel.

10
11 34. (Original) The computer-implemented method of claim 30 further
12 comprising:

13 storing the at least one random key in the main memory; and

14 locking the at least one random key in the main memory so that it does not
15 get transferred to the second storage.

16
17 35. (Original) An operating system programmed with instructions
18 which, when implemented by the operating system, implement the method of
19 claim 30.

20
21 36. (Original) A system for use in protecting pageable information
22 comprising:

23 a memory having pageable and non-pageable pages; and

24 at least one key stored in the memory in a non-pageable page, the key being
25 configured for use in encrypting pageable information.

1 37. (Original) The system of claim 36 further comprising a software
2 component that is configured to access and use said one key to encrypt pageable
3 information.

4
5 38. (Original) The system of claim 37, wherein the one key is accessible
6 only to the software component.

7
8 39. (Original) The system of claim 37 further comprising at least one
9 application configured to call the software component to encrypt the pageable
10 information.

11
12 40. (Original) The system of claim 37 further comprising a memory
13 manager configured to call the software component to encrypt the pageable
14 information.

15
16 41. (Original) A computer program embodied on one or more computer-
17 readable media, the program comprising:

18 encrypting information with a key that is page-locked in main memory of a
19 computer;

20 paging out, to secondary storage, the encrypted information;

21 accessing the encrypted information in the secondary storage; and

22 decrypting the encrypted information with the key that is page-locked in the
23 main memory.

24
25 42. (Original) A programmable computer comprising:
a processor;

1 main memory for holding information;
2 secondary storage for receiving information that is temporarily transferred
3 out of the main memory;
4 the computer being programmed with computer-readable instructions
5 which, when executed by the processor, cause the computer to:
6 encrypt information that is to be transferred to the secondary storage with a
7 key that is locked in the main memory;
8 transfer the encrypted information to the secondary storage; and
9 decrypt the encrypted information with a key that is locked in the main
10 memory.

11
12 43. (Original) The programmable computer of claim 42, wherein the
13 instructions cause the computer to generate the key and lock the key in the main
14 memory.

15
16 44. (Original) The programmable computer of claim 42, wherein the key
17 that is used to encrypt the information is the same key that is used to decrypt the
18 information.

19
20 45. (Original) The programmable computer of claim 42, further
21 comprising a software component that is programmed to encrypt and decrypt the
22 information.

23
24 46. (Original) The programmable computer of claim 45, wherein the
25 software component comprises the operating system's kernel.

1 47. (Original) One or more application programming interfaces
2 embodied on one or more computer-readable media for execution on a computer
3 in conjunction with a paging operating system having main memory for holding
4 information and a page file for receiving information that is paged out from the
5 main memory, comprising:

6 an interface method for encrypting pageable information with a key that is
7 page-locked in the main memory; and

8 an interface method for decrypting encrypted information that is contained
9 in the page file.
10

11 48. (Original) An application programming interface embodied on a
12 computer-readable medium for execution on a computer in conjunction with a
13 paging operating system having main memory for holding information and
14 secondary storage comprising a page file for receiving information that is paged
15 out from the main memory, comprising a method for setting an attribute on a page
16 of main memory, the attribute designating that the page must be encrypted with a
17 key that is page-locked in the main memory prior to the page being paged out to
18 the page file.
